Generators of the group of modular units for $\Gamma^1(N)$ over $\mathbf{Q}$

Marco Streng*

March 30, 2015

Abstract

We give two explicit sets of generators of the group of functions over $\mathbf{Q}$ on the modular curve $X^1(N)$ supported on the cusps.

The first set of generators is essentially the set of defining equations of $X^1(n)$ for $n \leq N/2$. It satisfies the same recurrence relation as the elliptic division polynomials, so this set of algebraic functions can be written down explicitly. Our result proves a conjecture of Maarten Derickx and Mark van Hoeij.

The second set of generators is explicit in terms of classical analytic functions known as Siegel functions.

Our proof consists of two parts. First, we relate our two sets of generators. Second, we use q-expansions and Gauss' lemma for power series to prove that our functions generate the full group of modular functions. The second part of the proof is partially inspired by a proof of Kubert and Lang.

1 Introduction

Let $N \geq 1$ be an integer. The modular curve $Y^1(N)$ is a smooth, affine, geometrically irreducible algebraic curve over $\mathbf{Q}$ and is often denoted $Y_1(N)$. It has the following property. For every field k of characteristic zero, if $N \geq 4$ or k is algebraically closed, then we have

$$Y^1(N)(k) = \{(E, P) : E \text{ is an elliptic curve over } k \text{ and } P \in E(k) \text{ has order } N\}/\cong .$$

Here we write $(E_1, P_1) \cong (E_2, P_2)$ when there is an isomorphism $\phi : E_1 \to E_2$ with $\phi(P_1) = P_2$. The equality "=" is a functorial Galois-equivariant bijection, which we use to identify the left and right hand side.

Our object of study is the group of *modular units on* $Y^1(N)$, that is, the unit group $\mathcal{O}(Y^1(N))^*$ of the ring $\mathcal{O}(Y^1(N))$ of regular functions over $\mathbf{Q}$ on $Y^1(N)$. The curve $Y^1(N)$ has a smooth compactification $X^1(N)$, and the group $\mathcal{O}(Y^1(N))^*$ equals the group of meromorphic functions over $\mathbf{Q}$ on $X^1(N)$ supported at the set $X^1(N) \setminus Y^1(N)$ of *cusps*.

*Universiteit Leiden, supported by NWO Vernieuwingsimpuls. The author would like to thank Peter Bruin, Maarten Derickx, Pınar Kılıçer and Mark van Hoeij for useful discussions.

The *Tate normal form* (Section 2.1) gives embeddings $Y^1(N) \hookrightarrow \mathbf{A}^2$ for all $N \geq 4$, and our first main result is as follows.

Theorem 1.1 (Conjecture 1 of [2])**.** *For all $n \geq 4$, let F_n be the defining polynomial of $Y^1(n)$ inside $\mathbf{A}^2$ as above. Then for all $N \geq 4$, the group $\mathcal{O}(Y^1(N))^*$ is $\mathbf{Q}^*$ times the free abelian group on $B, D, F_4, F_5, \ldots, F_{\lfloor N/2 \rfloor + 1}$ for explicit polynomials B and D.*

The polynomials B and D are given in Lemma 2.1, and it is known that the functions F_n can be explicitly given in terms of a recurrence relation, which we will recall in Remark 2.9. The main theorem therefore gives the group $\mathcal{O}(Y^1(N))^*$ very explicitly.

We prove the main theorem using modular forms over $\mathbf{C}$. Let $\mathbf{H} \subset \mathbf{C}$ be the standard upper half plane, $\mathbf{H}^* = \mathbf{H} \cup \mathbf{P}^1(\mathbf{Q}) \subset \mathbf{P}^1(\mathbf{C})$, and

$$\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : b \equiv 0, a \equiv d \equiv 1 \bmod N \right\}.$$

Recall the natural complex analytic isomorphism

$$\begin{aligned} \Gamma^1(N)\backslash\mathbf{H} &\longrightarrow Y^1(N)(\mathbf{C}) \\ \tau &\longmapsto (\mathbf{C}/\Lambda_\tau, \tau/N \bmod \Lambda_\tau), \end{aligned}$$

where $\Lambda_\tau = \tau\mathbf{Z} + \mathbf{Z}$. The functions on $X^1(N)$ defined over $\mathbf{Q}$ correspond exactly to the meromorphic functions on $\Gamma^1(N)\backslash\mathbf{H}$ whose q-expansions ($q = \exp(2\pi i\tau)$) are *rational*, that is, are in $\mathbf{Q}((q^{1/N}))$.

The group $\mathcal{O}(Y^1(N))^*$ equals the group of meromorphic functions on $\Gamma^1(N)\backslash\mathbf{H}^*$ supported on $\mathbf{P}^1(\mathbf{Q})$ with rational q-expansion.

Remark 1.2. Rationality of q-expansions is the reason for using the notation $Y^1(N)$ instead of the commonly used notation $Y_1(N)$ for the same curve over $\mathbf{Q}$. Had we used the group $\Gamma_1(N)$ (defined by $c \equiv 0$ rather than $b \equiv 0$) and $P = (1/N \bmod \tau)$ to give the complex uniformisation of our modular curve, then the field of functions defined over $\mathbf{Q}$ would not have corresponded to the field of functions with rational q-expansion at the cusp at infinity, but to the field of functions with rational expansion at the cusp zero (that is, a rational "$\exp(-2\pi i\tau^{-1})$-expansion").

Our second main result is the following, which is a strengthening of a specialisation of a result of Kubert and Lang [7, Theorems 1 and 2]. For $a \in \mathbf{Q}^2 \setminus \mathbf{Z}^2$, let h_a be the Siegel function as defined in Section 2.2 below.

Theorem 1.3. *Let*

$$S = \left\{ \prod_{k=1}^{\lfloor N/2 \rfloor} h_{(k/N,0)}^{e(k)} : \begin{array}{rcl} \forall_k \ e(k) & \in & \mathbf{Z}, \\ \sum_k e(k) & \in & 12\mathbf{Z}, \\ \sum_k k^2 e(k) & \in & \gcd(N,2)N\mathbf{Z} \end{array} \right\}.$$

Then S is free abelian of rank $\lfloor N/2 \rfloor$ and satisfies $\mathbf{Q}^* \times S = \mathcal{O}(Y^1(N))^*$.

1.1 Overview and methods

Our proof consists of two parts. The first part is Section 3, which relates the functions of Theorems 1.1 and 1.3 via explicit expressions in both directions. This is based on formulas from the theory of elliptic divisibility sequences that relate division polynomials with the Weierstrass sigma function.

The second part is Section 4, in which we show that our functions indeed generate the full group. As in Kubert-Lang [7], one of the key ideas is to use the fact that the space of modular forms of any given weight and level is generated by modular forms with integer coefficients. Together with Gauss' Lemma for power series with bounded denominator, this will show that if g^l is in our group for a modular function g, then so is g itself. We show that this idea works even better in the case of $\Gamma^1(N)$ over $\mathbf{Q}$ than in the case of [7], yielding results that are less general, but stronger, simpler and more elegant than the results of [7]. A detailed overview of this part of the proof is given at the beginning of Section 4.

Before we start the proof, Section 2 gives the functions appearing in both Theorems 1.1 and 1.3 and states more precise versions of Theorem 1.1.

2 The functions appearing in the main results

2.1 The Tate normal form

Let E be an elliptic curve over a field k and $P \in E(k)$ a point of order > 3 (possibly non-torsion).

Lemma 2.1 (Tate normal form)**.** Every pair (E, P) as above is isomorphic to a unique pair of the form

$$E : Y^2 + (1-C)XY - BY = X^3 - BX^2, \quad P = (0,0) \tag{1}$$

for $B, C \in k$ with

$$D := B^3 \cdot (C^4 - 8BC^2 - 3C^3 + 16B^2 - 20BC + 3C^2 + B - C) \neq 0.$$

Conversely, for every pair $B, C \in k$ with $D \neq 0$, equation (1) gives a pair (E, P).

Proof. Given (E, P), start with a general Weierstrass equation

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6. \tag{2}$$

As P does not have order 1, it is affine, and we translate P to $(0,0)$ yielding $A_6 = 0$. As P does not have order 2, we have $A_3 \neq 0$, and we add $(A_4/A_3)X$ to Y to get $A_4 = 0$. As P does not have order 3, we get $A_2 \neq 0$, and we scale X and Y to get $A_2 = A_3$. Then we define $C = 1 - A_1$ and $B = -A_2 = -A_3$. This uses up all freedom for changing Weierstrass equations [9, III.3.1(b)], so this form is uniquely defined. The quantity D is the discriminant of E, which is non-zero.

Conversely, if D is non-zero, then (E, P) defines an elliptic curve and a point on it, where the point does not have order 1, 2 or 3. □

For any curve E given by a general Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and any $n \in \mathbf{Z}$, the *n-division polynomial* ψ_n is given by

$$\begin{aligned}
\psi_0 &= 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2y + a_1x + a_3, \\
\psi_n &= \psi_{\gcd(n,2)} \cdot \prod_{Q \in (E[n] \setminus E[2])/\pm} (x - x(Q)) \qquad \text{if } n > 0, \\
\psi_{-n} &= -\psi_n.
\end{aligned}$$

For any non-singular point P on E, we have $nP = 0$ if and only if $\psi_n(P) = 0$.

Let $P_n \in \mathbf{Z}[B, C]$ be the n-division polynomial ψ_n of the elliptic curve (1) evaluated in the point $P = (0, 0)$. In particular, if $n \geq 4$ and (E, P) corresponds to $(B, C) \in k^2$ with $B \neq 0$, then $P \in E(k)$ has order dividing n if and only if $P_n(B, C) = 0$.

Example 2.2. For positive integers n, the n-division polynomial is computed by Sage [10] with the command

```
E.division_polynomial(n, two_torsion_multiplicity=1)
```

(implemented by David Harvey and John Cremona using formulas similar to those of Remark 2.9 below). We get the following list.

$$\begin{aligned}
P_1 &= 1 \\
P_2 &= (-1) \cdot B \\
P_3 &= (-1) \cdot B^3 \\
P_4 &= C \cdot B^5 \\
P_5 &= (-1) \cdot (-B + C) \cdot B^8 \\
P_6 &= (-1) \cdot B^{12} \cdot (C^2 - B + C) \\
P_7 &= B^{16} \cdot (C^3 - B^2 + BC) \\
P_8 &= C \cdot B^{21} \cdot (BC^2 - 2B^2 + 3BC - C^2)
\end{aligned}$$

For $n \geq 4$, let $F_n \in \mathbf{Z}[B, C]$ be P_n with all factors in common with D and P_d for $d < n$ removed (well-defined up to $\mathbf{Q}^*$). Following [2], we let $F_3 = B \in \mathbf{Z}[B, C]$ and $F_2 = B^4/D \in \mathbf{Q}(B, C)$.

Example 2.3.

$$\begin{aligned}
F_2 &= B \cdot (C^4 - 8BC^2 - 3C^3 + 16B^2 - 20BC + 3C^2 + B - C)^{-1} \\
F_3 &= B \\
F_4 &= C \\
F_5 &= C - B \\
F_6 &= C^2 - B + C \\
F_7 &= C^3 - B^2 + BC \\
F_8 &= BC^2 - 2B^2 + 3BC - C^2
\end{aligned}$$

For $N \geq 4$, the point $P = (0,0)$ on E is of order N if and only if $F_N = 0$. In particular, we recover the following known model of $Y^1(N)$.

Proposition 2.4. Let $R = \mathbf{Q}[B, C, D^{-1}] \subset \mathbf{Q}(B, C)$ and $\mathrm{Spec}(R/F_N) \subset \mathrm{Spec}(R) \subset \mathbf{A}^2$. Then for all $N \geq 4$ and all fields k of characteristic 0, we have $Y^1(N)(k) = \mathrm{Spec}(R/F_N)(k)$. □

In fact, when being more careful, one could even make this into a model of $Y^1(N)$ over $\mathbf{Z}[1/N]$, see [5, Corollary 45].

Corollary 2.5. For $N \geq 4$, F_N is an irreducible polynomial, and for $N \geq 2$, it coincides with F_N of Derickx and Van Hoeij [2].

Proof. For $N \in \{2, 3\}$, we used the definition of [2]. For $N \geq 4$, they define F_N by Proposition 2.4, and it is irreducible as $Y^1(N)$ is. □

Let $N \geq 4$ be an integer. In the previous section, we found a model for $Y^1(N)$ given by the equation $F_N = 0$ inside the surface A. In particular, by taking B, C, D, F_k and P_k modulo F_N, we get modular functions b, c, d, f_k and p_k on $Y^1(N)$ for all $k, N \in \mathbf{Z}$ with $k \geq 2$ and $N \geq 4$. Derickx and Van Hoeij show that they are *modular units*, that is, functions with divisors supported at the cusps. Let $\mathcal{O}(Y^1(N))^* \subset \mathbf{Q}(X^1(N))^*$ be the group of modular units. Our main result is the following.

Theorem 2.6 (aka Theorem 1.1 above, aka Conjecture 1 of [2])**.** *The group $\mathcal{O}(Y^1(N))^*/\mathbf{Q}^*$ is the free abelian group on $f_2, f_3, f_4, \ldots, f_{\lfloor N/2 \rfloor + 1}$.*

Before we start the proof, we rewrite the theorem in terms of p_n using the following lemma.

Lemma 2.7. For all $n \geq 3$, we have $\langle F_2, F_3, \ldots, F_n \rangle \times \mathbf{Q}^* = \langle B, D, P_4, P_5, \ldots, P_n \rangle \times \mathbf{Q}^*$.

Proof. Let G_n be the left hand side and H_n the left. We prove by induction on n that we have $G_n = H_n$ and that all irreducible factors of P_d for $d \leq n$ are in G_n.

For $n = 3$, we have $F_3 = B$ and $F_2 = B^4/D$ by definition, hence also $D = B^4/F_2$. As B and $D/B^3 = F_2^{-1}F_3$ are irreducible, the induction hypothesis follows for $n = 3$.

Suppose now that the induction hypothesis holds for $n = k-1$. By definition F_k is P_k except for factors in common with D and P_d for $d < k$, but by the induction hypothesis all such factors are in $G_{k-1} = H_{k-1}$. In particular, we get $G_k = H_k$. As F_k is irreducible by Corollary 2.5, we get the result. □

By Lemma 2.7, we find that Theorem 2.6 is equivalent to the following.

Theorem 2.8. *The group $\mathcal{O}(Y^1(N))^*/\mathbf{Q}^*$ is the free abelian group on b, d, $p_4, p_5, \ldots, p_{\lfloor N/2 \rfloor + 1}$.*

Remark 2.9. The division polynomials ψ_n, and hence our polynomials P_n and our functions p_n, satisfy the following recurrence relation. For all $m, n, k \in \mathbf{Z}$, we have

$$\psi_{m+n}\psi_{m-n}\psi_k^2 = \psi_{m+k}\psi_{m-k}\psi_n^2 - \psi_{n+k}\psi_{n-k}\psi_m^2.$$

Taking $(k,m,n) = (1,l+1,l)$ or $(1,l+1,l-1)$, we get

$$\begin{aligned}\psi_{2l+1} &= \psi_{l+2}\psi_l^3 - \psi_{l+1}^3\psi_{l-1},\\ \psi_{2l} &= \psi_2^{-1}\psi_l\left(\psi_{l+2}\psi_{l-1}^2 - \psi_{l-2}\psi_{l+1}^2\right),\end{aligned}$$

which gives p_n for all $n \geq 5$ starting from the initial terms p_1, p_2, p_3, p_4 of Example 2.2.

Example 2.10. The curve $X^1(5)$ is defined by $0 = F_5 = C - B$, that is, by $B = C$. We compute

$$\begin{array}{lcl} p_1 & = & 1 \\ p_2 & = & -c \\ p_3 & = & -c^3 \\ p_4 & = & c^6 \\ p_5 & = & 0 \\ p_6 & = & -c^{14} \\ p_7 & = & c^{19} \\ p_8 & = & c^{25} \\ p_9 & = & -c^{32} \\ p_{10} & = & 0 \\ d & = & c^5\cdot(c^2-11c-1), \end{array}$$

which indeed all lie in the group generated by $b = c$ and d.

Example 2.11. The curve $X_1(6)$ is defined by $0 = f_6 = C^2 - B + C$, that is, by $B = C(C+1)$. We compute

$$\begin{array}{lcl} p_1 & = & 1 \\ p_2 & = & -c \cdot(c+1) \\ p_3 & = & -c^3 \cdot(c+1)^3 \\ p_4 & = & c^6 \cdot(c+1)^5 \\ p_5 & = & c^{10}\cdot(c+1)^8 \\ p_6 & = & 0 \\ p_7 & = & -c^{20}\cdot(c+1)^{16} \\ p_8 & = & -c^{26}\cdot(c+1)^{21} \\ p_9 & = & c^{33}\cdot(c+1)^{27} \\ p_{10} & = & c^{41}\cdot(c+1)^{33} \\ d & = & c^6 \cdot(c+1)^3\cdot(9c+1), \end{array}$$

which indeed all lie in the group generated by $b = c(c+1)$, d and p_4.

2.2 Siegel functions

This section defines the *Siegel functions* of Theorem 1.3 and recalls their transformation properties and q-expansions. Our main reference for this section is Fricke [4]. We start by recalling the well-known Weierstrass sigma function and Dedekind eta function.

2.2.1 Lattices, sigma and eta

By a *lattice*, we will always mean a discrete subgroup $\Lambda \subset \mathbf{C}$ of rank 2. For example, for $\tau \in \mathbf{H}$, we have a lattice $\Lambda_\tau = \tau\mathbf{Z} + \mathbf{Z}$. For $\omega_1, \omega_2 \in \mathbf{C}$ with $\tau = \omega_1/\omega_2 \in \mathbf{H}$, we have a lattice $\omega_1\mathbf{Z} + \omega_2\mathbf{Z} = \omega_2\Lambda_\tau$.

We define the *Weierstrass sigma function* by ([4, (1) on p.258])

$$\sigma(z,\Lambda) = z \prod_{\substack{w\in\Lambda \\ \omega\neq 0}} (1-\frac{z}{w}) \exp\left(\frac{z}{w} + \frac{1}{2}(\frac{z}{w})^2\right)$$

for all $z \in \mathbf{C}$ and all lattices $\Lambda \subset \mathbf{C}$. We also define $\sigma(z,\tau) = \sigma(z,\Lambda_\tau)$.

Let $\zeta(z,\Lambda) = \frac{\frac{d}{dz}\sigma(z,\Lambda)}{\sigma(z,\Lambda)}$ be the logarithmic derivative of σ ([4, (6) on p.209]). Is is quasi-periodic in the sense that we have

$$\zeta(z+\omega_i,\Lambda) = \zeta(z,\Lambda) + \eta_i,$$

for some $\eta_1, \eta_2 \in \mathbf{C}$, which we call the *basic quasi periods* associated to ω_1, ω_2 [4, (4) on p.196]. They satisfy the Legendre relation $\omega_1\eta_2 - \omega_2\eta_1 = 2\pi i$ ([4, (6) on p.160]).

Let η (not to be confused with η_1 and η_2) be the *Dedekind eta function*

$$\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) \qquad \text{where} \qquad q = \exp(2\pi i\tau).$$

2.2.2 Klein forms and Siegel functions

For $a = (a_1, a_2) \in \mathbf{Q}^2 \setminus \mathbf{Z}^2$ and $\Lambda = \omega_1\mathbf{Z} + \omega_2\mathbf{Z}$, define the *Klein form*

$$\mathfrak{t}_a(\omega_1,\omega_2) = \exp\left(-\tfrac{1}{2}(a_1\eta_1 + a_2\eta_2)(a_1\omega_1 + a_2\omega_2)\right)\sigma\left(a_1\omega_1 + a_2\omega_2, \Lambda\right).$$

Our Klein form equals $-\sigma_{gh}(\omega_1,\omega_2)$ in the notation of [4, (6) on p.451] where $(g/n, h/n) = a$.

Define for $a = (a_1, a_2) \in \mathbf{Q}^2 \setminus \mathbf{Z}^2$ the function

$$\mathfrak{t}_a(\tau) = \omega_2^{-1}\mathfrak{t}_a(\omega_1,\omega_2), \tag{3}$$

which by [4, (7) on p.452] depends only on a and $\tau = \omega_1/\omega_2 \in \mathbf{H}$, not on ω_1 and ω_2.

Define the *Siegel function*

$$h_a = 2\pi\eta^2\mathfrak{t}_a.$$

Remark 2.12. Our Klein forms and Siegel functions are the same as those in Kubert and Lang [6, 7] up to multiplication by a constant and taking fractional powers. Kubert and Lang do not have the factor $\frac{1}{2}$ in the exponent in the definition of $\mathfrak{t}_a(\omega_1,\omega_2)$ ([6, p.176]), but this is either due to a typo in [6] or due to different scaling conventions on e.g. ω_i and/or η_i. Indeed, the definition as we have given it satisfies [6, K2 on p.177], and it would not have done so without the factor $\frac{1}{2}$.

The notation of Kubert and Lang varies a bit from paper to paper. For details of the relations between the functions, see the following equalities, where a superscript II refers to [6] and IV to [7]. Moreover, in the case of II, a positive integer N is understood to be fixed and we have $a = (r/N, s/N)$. Up to constant factors, we have

$$\begin{array}{rclcl} \mathfrak{t}_a & = & \mathfrak{t}^{\mathrm{II}}_{r,s} & = & \mathfrak{t}^{\mathrm{IV}}_a, \\ h_a & = & (g^{\mathrm{II}}_{r,s})^{1/(12N)} & = & h^{\mathrm{IV}}_a \quad = \quad \begin{cases} g^{\mathrm{IV}}_a & \text{if } 2a \notin \mathbf{Z}^2, \\ (g^{\mathrm{IV}}_a)^2 & \text{if } 2a \in \mathbf{Z}^2. \end{cases} \end{array}$$

Lemma 2.13. The Siegel functions h_a have the following expansions and transformation properties for all $a = (a_1, a_2) \in \mathbf{Q}^2 \setminus \mathbf{Z}$.

1. Write $q^a = \exp(2\pi i a_2) q^{a_1}$. If $0 \le a_1 \le \frac{1}{2}$, then we have
$$h_a = c(a) q^{\frac{1}{2}(a_1^2 - a_1 + \frac{1}{6})} (1 - q^a) \prod_{n=1}^{\infty} (1 - q^n q^a)(1 - q^n q^{-a}), \tag{4}$$
where $c(a) = i \exp(\pi i a_2 (a_1 - 1))$ is a constant.
2. $h_{-a} = -h_a$.
3. $h_{(a_1+n_1, a_2+n_2)} = (-1)^{n_1 n_2 + n_1 + n_2} e^{-\pi i (n_1 a_2 - n_2 a_1)} h_{(a_1, a_2)}$ for all $(n_1, n_2) \in \mathbf{Z}^2$,
4. $h_{(a_1+1, 0)} = -h_{(a_1, 0)}$.
5. h_a up to multiplication by roots of unity depends only on the class of a in $(\mathbf{Q}^2/\mathbf{Z}^2)/\{\pm 1\}$.
6. For all
$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}),$$
we have
$$h_a(M\tau) = \epsilon(M) h_{aM}(\tau), \tag{5}$$
where $\epsilon(M) \in \mathbf{C}^*$ is such that for all $\tau \in \mathbf{H}$,
$$\eta(M\tau)^2 = \epsilon(M)(\gamma\tau + \delta)\eta(\tau)^2. \tag{6}$$
7. The function ϵ from the previous point satisfies $\epsilon(M)^{12} = 1$ and
$$\epsilon\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = \exp(2\pi i/12)^{-1}.$$

Proof. The expansion in 1. is Fricke [4, (7) on p.452], but note that our q is the square of the q of Fricke. Equivalently, the expansion is $-i$ times Kubert and Lang [6, K5 on p.178].

The identity $h_{-a} = -h_a$ of 2. follows from the anti-symmetry of σ as a function of z.

The identity of 3. is Fricke [4, (4) on p.451]. Identity 4. is a special case of 3.

Observation 5. follows immediately from 2. and 3..

As η^{24} has level 1, if we let $\epsilon(M, \tau) = \eta(M\tau)^2/((\gamma\tau + \delta)\eta(\tau)^2)$, then we get $\epsilon(M, \tau)^{12} = 1$, hence $\epsilon(M, \tau)$ is independent of τ, call it $\epsilon(M)$. A numerical evaluation yields the example value of 7., so it remains to prove equality (5) in 6.

First, [4, (3) on p.451] (equivalently [6, K1 on p.177]) gives
$$\mathfrak{t}_a(M \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}) = \mathfrak{t}_{aM}(\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}).$$
In terms of $\tau = \omega_1/\omega_2$, this reads (by (3))
$$(\gamma\omega_1 + \delta\omega_2)\mathfrak{t}_a(M\tau) = \omega_2 \mathfrak{t}_{aM}(\tau).$$

Now multiply this equality by 2π and (6) to get

$$(\gamma\omega_1 + \delta\omega_2)h_a(M\tau) = (\gamma\tau + \delta)\omega_2\epsilon(M)h_{aM}(\tau),$$

which proves (5). □

3 Relating the functions

We now give the first part of the proof of the main theorems: relating the groups given by the sets of generators of the theorems. We start by expressing the functions P_n and p_n of Section 2.1 in terms of the Weierstrass σ-function.

3.1 The Weierstrass sigma function

To any lattice $\Lambda \subset \mathbf{C}$ of rank two and any $z \in \mathbf{C}$, we associate the elliptic curve E with $E(\mathbf{C}) = \mathbf{C}/\Lambda$ and the point $P = (z \bmod \Lambda) \in E(\mathbf{C})$. After putting the pair (E, P) in Tate normal form, we get B and C as functions in z and Λ. In particular, we get expressions for P_n in terms of z and Λ. The following result gives these expressions.

Let $\Delta = \Delta(\Lambda)$ be the discriminant of the classical Weierstrass equation

$$W : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda). \tag{7}$$

Proposition 3.1. Let

$$\Phi_n = \frac{\sigma(nz, \Lambda)}{\sigma(z, \Lambda)^{n^2}} \quad \text{and} \quad U = \Phi_3/(\Phi_2)^3.$$

Then we have for all integers n

$$P_n = U^{n^2-1}\Phi_n \quad \text{and} \quad D = U^{12}\Delta.$$

Proof. Let $\wp(z, \Lambda)$, $g_2(\Lambda)$, $g_3(\Lambda)$ be the usual Weierstrass functions and $\wp' = \frac{d}{dz}\wp$. Then for any $v \in \mathbf{C}$, we get a point $(x, y) = (\wp(v, \Lambda), \wp'(v, \Lambda))$ on (7).

We put the classical Weierstrass equation W in Tate normal form relative to the point $P = (x_0, y_0) = (\wp(z, \tau), \wp'(z, \tau))$. The transformation is of the form $X = u^2(x + t)$, $Y = \frac{1}{2}u^3(y + rx + s)$ with u, r, s, t functions of z and τ.

First, we compute the discriminant D of the Tate normal form. Note that the discriminant of the elliptic curve $y^2 = f(x)$ is 16 times the discriminant of the polynomial $f(x)$. We get

$$\begin{aligned} D &= -16 \prod_{Q_1 \neq Q_2 \in E[2]\setminus\{0\}} (X(Q_1) - X(Q_2)) \\ &= -16u^{12} \prod_{Q_1 \neq Q_2 \in E[2]\setminus\{0\}} (x(Q_1) - x(Q_2)) \\ &= u^{12}\Delta. \end{aligned}$$

Similarly, we compute

$$P_n = n\sqrt{\prod_{Q \in E[n]\setminus\{0\}} (X - X(Q))} = u^{(n^2-1)}n\sqrt{\prod_{Q \in E[n]\setminus\{0\}} (x - x(Q))},$$

where the square root is chosen to be a monic polynomial in X times 1 or times $Y + \frac{1}{2}a_1X + \frac{1}{2}a_3$. It is a classical fact that the following holds (for a proof, see Theorem 2.7 of Looij [1])

$$n^2 \prod_{Q \in E[n] \setminus \{0\}} (x - x(Q)) = \left(\sigma(nz, \Lambda)/\sigma(z, \Lambda)^{n^2}\right).$$

The proof works by fixing the lattice Λ and showing that both sides are elliptic functions for that lattice with the same divisor and with equal leading terms in their power series. Looking up the square root in [1], we find that it differs from ours by a factor $(-1)^{n+1}$. In particular, we get

$$P_n = (-u)^{n^2-1}\sigma(nz, \Lambda)/\sigma(z, \Lambda)^{n^2} = (-u)^{n^2-1}\Phi_n, \tag{8}$$

so it suffices to prove $u = -U$.

Proving $u = -U$ could be done by a lengthy computation of the Tate normal form from W. Instead, simply note

$$1 = \frac{B^3}{B^3} = \frac{P_3}{P_2^3} = \frac{(-u)^{3^2-1}}{(-u)^{3(2^2-1)}}\frac{\Phi_3}{\Phi_2^3} = (-u)^{-1}U,$$

which finishes the proof. □

There is a natural complex analytic isomorphism $\Gamma^1(N)\backslash\mathbf{H} \to Y^1(N)$ given by sending $\tau \in \mathbf{H}$ to $(\mathbf{C}/\Lambda_\tau, \tau/N \bmod \Lambda_\tau)$, so we interpret functions on $Y^1(N)$ as functions on $\mathbf{H}$. We then have the following.

Corollary 3.2. Let

$$\phi_n = \frac{\sigma\left(\frac{n\tau}{N}, \tau\right)}{\sigma\left(\frac{\tau}{N}, \tau\right)^{n^2}} \quad \text{and} \quad u = \phi_3/(\phi_2)^3.$$

Then for all integers $N \geq 4$ and $n \in \mathbf{Z}$ the following identities of meromorphic functions hold on $X_1(N)$:

$$p_n = u^{n^2-1}\phi_n \quad \text{and} \quad d = (2\pi\eta^2 u)^{12}.$$

Proof. Take $\Lambda = \Lambda_\tau$ and $z = \tau/N$ in Proposition 3.1, and use the well known fact that $\Delta(\Lambda_\tau) = (2\pi\eta(\tau)^2)^{12}$ □

3.2 The functions p_n in terms of h_a and vice versa

Now that we have expressed the functions p_n in terms of Weierstrass σ-functions, we use these expressions to express the p_n in terms of Siegel functions and to express Siegel functions in terms of the functions p_n.

Lemma 3.3. Let

$$t = \frac{h_{(1/N,0)}^2 h_{(3/N,0)}}{h_{(2/N,0)}^3}.$$

Then for all integers $N \geq 4$ and n we have

$$p_n = t^{n^2-1}\frac{h_{(n/N,0)}}{h_{(1/N,0)}} \quad \text{and} \quad d = (th_{(1/N,0)})^{12} \quad \text{on } X^1(N).$$

Proof. In the notation of Corollary 3.2, we have

$$\begin{aligned}
\phi_n &= \frac{\sigma(n\tau/N,\tau)}{\sigma(\tau/N,\tau)^{n^2}} = \frac{\mathfrak{t}_{(n/N,0)}}{\mathfrak{t}_{(1/N,0)}^{n^2}} = \frac{h_{(n/N,0)}}{h_{(1/N,0)}^{n^2}}(2\pi\eta^2)^{n^2-1} \\
&= \frac{h_{(n/N,0)}}{h_{(1/N,0)}}\left(\frac{h_{(1/N,0)}}{2\pi\eta^2}\right)^{1-n^2}, \\
u &= \phi_3\phi_2^{-3} = t\cdot\left(\frac{h_{(1/N,0)}}{2\pi\eta^2}\right), \\
p_n &= u^{n^2-1}\phi_n = t^{n^2-1}\frac{h_{(n/N,0)}}{h_{(1/N,0)}}, \\
d &= \left(2\pi\eta^2 u\right)^{12} = (th_{(1/N,0)})^{12},
\end{aligned}$$

so the result follows. □

Let $m = \lfloor N/2 \rfloor$. Next, we express p_{m+1} in terms of $h_{(k/N,0)}$ with $1 \le k \le m$ using the periodicity and symmetry of $h_{(k/N,0)}$ in k.

Lemma 3.4. Let t be as in Lemma 3.3, let $m = \lfloor N/2 \rfloor$, and let $v = t^{\gcd(2,N)N}$. Then we have

$$p_{m+1} = \begin{cases} vp_m, & \text{if } N \text{ is odd,} \\ vp_{m-1}, & \text{if } N \text{ is even.} \end{cases}$$

Moreover, each of $d, -b = p_2, p_4, p_5, p_6, \ldots, p_{m+1}$ is of the form

$$f = \prod_{k=1}^{m} h_{(k/N,0)}^{e(k)},$$

where for every $k \in \{1, 2, \ldots, m\}$ we have $e(k) \in \mathbf{Z}$, and where we have

$$\sum_{k=1}^{m} e(k) \in 12\mathbf{Z} \qquad \text{and} \qquad \sum_{k=1}^{m} k^2 e(k) \in N\gcd(N,2)\mathbf{Z}. \tag{9}$$

Proof. Suppose first that N is odd, so $N = 2m+1$. Lemma 3.3 gives

$$p_{m+1} = t^{(m+1)^2-1} h_{((m+1)/N,0)}/h_{(1/N,0)}$$

and by Lemma 2.13.2 and .4, we have $h_{((m+1)/N,0)} = -h_{(-(m+1)/N,0)} = h_{(m/N,0)}$, hence

$$p_{m+1} = t^N t^{m^2-1} h_{(m/N,0)}/h_{(1/N,0)} = vp_m.$$

If N is even, then $N = 2m$ and $t^{(m+1)^2-1} = t^{2N}t^{(m-1)^2-1}$, so the same calculation gives $p_{m+1} = vp_{m-1}$.

A straightforward calculation verifies (9) for each expression in Lemma 3.3 or 3.4. Indeed, the value of $(\sum_k e(k), \sum_k k^2 e(k)) \in \mathbf{Z}^2$ is

$$\begin{aligned}
(1, k^2) &\qquad \text{for } h_{(k/N,0)}, \\
(0, -1) &\qquad \text{for } t, \\
(12, 0) &\qquad \text{for } d, \\
(0, 0) &\qquad \text{for } p_n \text{ with } 1 \le n \le m, \\
(0, -\gcd(N,2)N) &\qquad \text{for } v \text{ and hence for } p_{m+1}.
\end{aligned}$$

□

Now that we have expressions of p_n in terms of $h_{(k/N,0)}$, it is a matter of solving a system of linear equations to obtain the reverse expressions. These expressions are given in the following result.

Proposition 3.5. Given $e \in \mathbf{Z}^m$ satisfying (9) and given

$$f = \prod_{k=1}^{m} h_{(k/N,0)}^{e(k)},$$

let $\alpha = \frac{1}{12}\sum_k e(k)$ and $\beta = (N \gcd(2,N))^{-1} \sum_k k^2 e(k)$. Then we have

$$f = d^{\alpha} \left(p_{N-m-1} p_{m+1}^{-1}\right)^{\beta} \prod_{k=1}^{m} p_n^{e(k)}, \tag{10}$$

where $p_1 = 1$, $p_2 = -b$, $p_3 = -b^3$, and $N - m - 1 \in \{m-1, m\}$, so

$$f \in \langle -b, d, p_4, p_5, \ldots, p_{m+1} \rangle \subset \mathcal{O}(Y^1(N))^*.$$

Proof. Note that Lemma 3.3 gives

$$\prod_{k=1}^{m} p_n^{e(k)} = t^{\sum_k k^2 e(k)^2} (t h_{(1/N,0)})^{-\sum e(k)} \prod_{k=1}^{m} h_{(k/N,0)}^{e(k)} = v^{\beta} d^{-\alpha} \prod_{k=1}^{m} h_{(k/N,0)}^{e(k)}.$$

As Lemma 3.4 gives $v = p_{m+1} p_{N-m-1}^{-1}$, this proves (10). The formulas for p_1, p_2 and p_3 are in Example (2.2). □

Summary 3.6. Let S be the group of functions of the form $\prod_{k=1}^{m} h_{(k/N,0)}^{e(k)}$ satisfying (9). In order to prove Theorems 1.1, 1.3, 2.6 and 2.8, it suffices to prove that S has rank m and that $S \times \mathbf{Q}^*$ contains $\mathcal{O}(Y^1(N))^*$.

Proof. We have already established that the functions given in Theorems 1.1, 2.6 and 2.8 generate the same group $T \subset \mathcal{O}(Y^1(N))^*$ (see Lemma 2.7 and the paragraph above Theorem 2.6). Lemma 3.3 and Proposition 3.5 show that the group $S \times \mathbf{Q}^*$ of Theorem 1.3 is equal to the group $T \times \mathbf{Q}^*$, hence is contained in $\mathcal{O}(Y^1(N))^*$.

In order to prove in each of the four theorems that the given group equals $\mathcal{O}(Y^1(N))$ it now suffices to prove the other inclusion: $S \times \mathbf{Q}^* \supset \mathcal{O}(Y^1(N))$. And in order to prove for each of Theorems 1.1, 2.6 and 2.8 the that the m given functions generate a free group, it suffices to prove that S is free of rank m. □

4 Using the power series

Recall that S is the group of functions of the form $\prod_{k=1}^{m} h_{(k/N,0)}^{e(k)}$ satisfying (9), where $m = \lfloor N/2 \rfloor$. As stated in Summary 3.6, it now suffices to prove that S has rank m and $\mathcal{O}(Y^1(N))^* \subset S \times \mathbf{Q}^*$.

Section 4.1 uses q-expansions to show that the Siegel functions $h_{(k/N,0)}$ for $k = 1, 2, \ldots, m$ are multiplicatively independent. The group they generate then has the correct rank.

Section 4.2 combines the above with Gauss' Lemma for power series to show that $\mathcal{O}(Y^1(N))^*$ is contained in $\langle h_{(k/N,0)} : k = 1, 2, \ldots, m-1 \rangle \times \langle h_{(m/N,0)}^{1/2} \rangle \times \mathbf{Q}^*$.

Section 4.3 then finishes the proof of $\mathcal{O}(Y^1(N))^* \subset S \times \mathbf{Q}^*$ using explicit SL_2-actions.

4.1 The rank

Proposition 4.1. The functions $h_{(k/N,0)}$ for $k = 1, 2, \ldots, m$ are multiplicatively independent modulo $\mathbf{C}^*$. In other words, if we have

$$\prod_{k=1}^{m} h_{(k/N,0)}^{e(k)} \in \mathbf{C}^*$$

for any $e \in \mathbf{Z}^k$, then we have $e = 0$.

Proof. We prove the result using q-expansions. For $a = (a_1, a_2) \in \mathbf{Q}^2$, let $q^a = q^{a_1} \exp(2\pi i a_2)$. Recall from (4) that if $0 \le a_1 \le \frac{1}{2}$, then

$$h_a = q^{\frac{1}{2}(a_1^2 - a_1 + \frac{1}{6})}(1 - q^a) \prod_{n=1}^{\infty} (1 - q^n q^a)(1 - q^n q^{-a}).$$

If αq^r is the lowest term of a Laurent series f, then the *reduced form* of f is $f^* = f/(\alpha q^r)$. We compute

$$\begin{aligned} h^*_{(a_1,0)} &= 1 - q^{a_1} + O(q^{1-a_1}) \qquad \text{for } 0 < a_1 < \tfrac{1}{2}, \text{ and} \\ h^*_{(1/2,0)} &= 1 - 2q^{1/2} + O(q^{3/2}). \end{aligned} \tag{11}$$

It suffices to prove that the functions $h_{(k/N,0)}$ for $1 \le k \le m$ are multiplicative-linearly independent modulo $\mathbf{C}^*$. So suppose that we have $\prod_{k=1}^{m} h_{(k/N,0)}^{e(k)} \in \mathbf{C}^*$ for some $0 \ne e \in \mathbf{Z}^m$. Let k_0 be the smallest positive integer with $e(k_0) \ne 0$. Then (11) gives

$$1 = \prod_{k=k_0}^{m} (h^*_{(k/N,0)})^{e(k)} = \begin{cases} 1 - e(k_0) q^{k_0/N} + O(q^{(k_0+1)/N}) & \text{if } 2k_0 \ne N, \text{ and,} \\ 1 - 2e(k_0) q^{k_0/N} + O(q^{(k_0+1)/N}) & \text{if } 2k_0 = N. \end{cases}$$

We get $e(k_0) = 0$, contradiction. □

Corollary 4.2. Let S be the group of functions $\prod h_{(k/N,0)}^{e(k)}$ satisfying (9). Then the image of S in $\mathcal{O}(Y^1(N))^*/\mathbf{Q}^*$ has finite index.

Proof. Proposition 4.1 shows that S has rank m. We have

$$\operatorname{rk}(\mathcal{O}(Y^1(N))^*/\mathbf{Q}^*) \le \#\left(\{\text{cusps of } X^1(N)\}/\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\right) - 1.$$

As the right hand side is m by [2, footnote 4 on p.4], this proves the result. □

We recover the following consequence of the Manin-Drinfeld theorem [8, 3], which states that the cuspidal parts of modular Jacobians are torsion.

Corollary 4.3. The group

$$\frac{\operatorname{Div}^{0,\text{cusp}}(X^1(N))}{\mathcal{O}(Y^1(N))^*/\mathbf{Q}^*}$$

is finite.

Proof. As seen in the proof of Corollary 4.2, the two groups in the quotient both have rank m. □

4.2 Higher roots of power series

In the previous section, we have shown that every $f \in \mathcal{O}(Y^1(N))^*$ can be expressed as a product of powers $c\prod_{k=1}^m h_{(k/N,0)}^{e(k)}$ with $e \in \mathbf{Q}^m$ and $c \in \mathbf{C}^*$. The current section is devoted to proving that the exponent $e(k)$ is an integer for $k \neq N/2$. The key idea, taken from Kubert and Lang [7] is to combine Gauss' lemma for power series with the fact that q-expansions of modular forms have bounded denominators.

We call a power series $f \in \mathbf{Z}[[x]]$ *primitive* if the ideal generated by its coefficients is (1). We then have the following variant of Gauss' lemma.

Lemma 4.4. Let $f, g \in \mathbf{Z}[[x]]$ be primitive power series. Then $fg \in \mathbf{Z}[[x]]$ is also primitive.

Proof. Given any prime number p, take the lowest-order terms of (f mod p) and (g mod p) (which exist by primitivity). Their product is a non-zero term of (fg mod p), so $p \nmid fg$. □

We say that a Laurent series $f \in \mathbf{Q}((x))$ has a *bounded denominator* if there is a non-zero $d \in \mathbf{Z}$ such that $df \in \mathbf{Z}((x))$.

Corollary 4.5. Let $f, g \in \mathbf{Q}[[x]]$ be power series with bounded denominator and constant term 1. If fg is in $\mathbf{Z}[[x]]$, then $f, g \in \mathbf{Z}[[x]]$.

Proof. Take $a, b \in \mathbf{Z}$ such that af and bg are primitive in $\mathbf{Z}[[x]]$. Then $(ab)(fg)$ is primitive by Lemma 4.4, hence $a, b \in \{\pm 1\}$. □

Proposition 4.6 (Special case of Lemma 3.1 of Kubert and Lang [7])**.** Let f be a modular unit with rational q-expansion, that is, in $\mathbf{Q}((q^{1/M}))$ for some M. Then the q-expansion has bounded denominator.

Proof. See [7, Lemma 3.1] for the proof, of which we give a sketch here. After multiplying by a power of η^{24}, the function becomes a cusp form. The vector space of cusp forms of given weight is generated by forms with *integer* Fourier expansions, hence the result follows. □

For a formal power series f with constant coefficient 1, we define $f^{a/b}$ to be the unique bth root of f^a with constant coefficient 1, and for a meromorphic function f on $\mathbf{H}$, we denote by $f^{a/b}$ any bth root of f^a.

Proposition 4.7. Suppose f is a *modular* function of any level and suppose that we have

$$f = c\prod_{k=1}^m h_{(k/N,0)}^{e(k)}$$

with $e \in \mathbf{Q}^m$ and $c \in \mathbf{C}^*$. Then for all k we have $e(k) \in \mathbf{Z}$ if $2k \neq N$ and $e(k) \in \frac{1}{2}\mathbf{Z}$ if $2k = N$.

Proof. Taking reduced forms on both sides, we get

$$(f^*)^n = \prod_{k=1}^m (h_{(k/N,0)}^*)^{n\cdot e(k)}$$

for some n with $ne \in \mathbf{Z}^m$. The right hand side has integer coefficients, so by Proposition 4.6 and Corollary 4.5, we find that f^* has integer coefficients.

We prove the result by induction on k. Suppose it is true for all $k < k_0$. Then we have

$$f^* \prod_{k=1}^{k_0-1} (h^*_{(k/N,0)})^{-e(k)} = \prod_{k=k_0}^{m} (h^*_{(k/N,0)})^{e(k)}.$$

The left hand side has integer coefficients. By the formula in the proof of Proposition 4.1, the right hand side is

$$1 = \prod_{k=k_0}^{m} (h^*_{(k/N,0)})^{e(k)} = \begin{cases} 1 - e(k_0)q^{k_0/N} + O(q^{(k_0+1)/N}) & \text{if } 2k_0 \neq N, \text{ and,} \\ 1 - 2e(k_0)q^{k_0/N} + O(q^{(k_0+1)/N}) & \text{if } 2k_0 = N. \end{cases}$$

Hence the result follows. □

4.3 Proof of the main theorems

Next, we use the action of SL_2. Note that by Summary 3.6 and Proposition 4.1, the following result finishes the proof of Theorems 1.1, 1.3, 2.6 and 2.8..

Theorem 4.8. *Let $f \in \mathcal{O}(Y^1(N))^*$. Then $f = c\prod_{k=1}^m h_{(k/N,0)}^{e(k)}$, where $c \in \mathbf{Q}^*$ and $e \in \mathbf{Z}^m$ are uniquely determined by f and satisfy* (9)*, that is,*

$$\sum_k e(k) \in 12\mathbf{Z} \qquad \text{and} \qquad \sum_k k^2 e(k) \in N \gcd(N,2)\mathbf{Z}.$$

Proof. By Corollary 4.2, we find that f can be written as $c\prod h_{(k/N,0)}^{e(k)}$ with $e(k) \in \mathbf{Q}$. Here c and e are uniquely determined by Proposition 4.1. Moreover, the numbers $e(1), e(2), \ldots, e(m-1)$ are in $\mathbf{Z}$ by Proposition 4.7. Next, we prove (9), which also implies $e(m) \in \mathbf{Z}$.

Consider the matrix

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \Gamma^1(N).$$

Then we have $f(M\tau) = f(\tau)$, so we inspect the action of M on the functions $h_{(k/N,0)}$. Lemma 2.13.6 and .7 gives $h_{(k/N,0)}(M\tau) = \exp(2\pi i/12)^{-1} h_{(k/N,0)}(\tau)$ for this matrix M. In particular, we get $\sum_k e(k) \in 12\mathbf{Z}$.

Next, consider the matrix

$$M = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma^1(N).$$

Again we have $f(M\tau) = f(\tau)$, that is, $f(M\tau) = f(\tau + N)$, which shows that the q-expansion of f is in $\mathbf{C}((q^{1/N}))$. In the product expansion (4), we consider the leading term $-iq^{\frac{1}{2}(a_1^2 - a_1 + \frac{1}{6})}$ (with $a_1 = k/N$) of $h_{(k/N,0)}$. As the leading term of f is a constant times a power of $q^{1/N}$, we get

$$\frac{1}{12N^2} \sum_{k=1}^{m} e(k)(6k^2 - 6kN + N^2) \in \frac{1}{N}\mathbf{Z}.$$

As we already have $\sum e(k) \in 12\mathbf{Z}$, we get

$$\sum_{k=1}^{m} e(k)(k^2 - kN) \in 2N\mathbf{Z} \subset N\mathbf{Z},$$

hence in particular $\sum e(k)k^2 \in N\mathbf{Z}$. If N is odd, then this finishes the proof. If N is even, then we get

$$\begin{aligned}(1-N)\sum_{k=1}^{m} e(k)k^2 &= \sum_{k=1}^{m} e(k)(k^2 - k^2N) \\ &\equiv \sum_{k=1}^{m} e(k)(k^2 - kN) \equiv 0 \bmod 2N\mathbf{Z},\end{aligned}$$

and since $N-1$ is coprime to $2N$, this proves (9) and hence $e(m) \in \mathbf{Z}$.

It remains to prove $c \in \mathbf{Q}^*$. Let $g = f/c$, which is in $\mathcal{O}(Y^1(N))^*$ by Proposition 3.5. Then $c = f/g$ is a constant in $\mathcal{O}(Y^1(N))^*$, hence is in $\mathbf{Q}^*$. □

References

[1] Rutger de Looij. Elliptic divisibility sequences, 2010. Master's thesis, Mathematical Sciences, Universiteit Utrecht, written under the supervision of Gunther Cornelissen, `http://dspace.library.uu.nl/bitstream/handle/1874/206176/LooijRutgerdeMA2010.pdf`.

[2] Maarten Derickx and Mark van Hoeij. Gonality of the modular curve $X_1(n)$. arXiv:1307.5719.

[3] V. G. Drinfeld. Two theorems on modular curves. *Funkcional. Anal. i Priložen.*, 7(2):83–84, 1973.

[4] Robert Fricke. *Die elliptischen Funktionen und ihre Anwendungen. Erster Teil. Die funktionentheoretischen und analytischen Grundlagen*. Springer, Heidelberg, 2011. Reprint of the 1916 original.

[5] Jinbi Jin. Homogeneous division polynomials for weierstrass elliptic curves. arXiv:1303.4327, 2013.

[6] Dan Kubert and Serge Lang. Units in the modular function field. II. A full set of units. *Math. Ann.*, 218(2):175–189, 1975.

[7] Daniel Kubert and Serge Lang. Units in the modular function field. IV. The Siegel functions are generators. *Math. Ann.*, 227(3):223–242, 1977.

[8] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[9] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[10] W. A. Stein et al. *Sage Mathematics Software (Version 6.2)*. The Sage Development Team, 2014. `http://www.sagemath.org`.